УДК: 004.7.056

DoS напади кај безжичните мрежи и методи за намалување на ефектите од овие напади

Елена Конеска, Јасминка Сукаровска Костадиновска, М-р Митко Богданоски, Доц. Д-р Сашо Гелев
Европски Универзитет – Скопје, Р. Македонија,
koneska.elena@live.eurm.edu.mk, sukarovska.jasminka@live.eurm.edu.mk, {mitko.bogdanoski, saso.gelev}@eurm.edu.mk

Апстракт – *DoS (Одбивање на Услуга) нападите се едни од најголемите закани на безжичните мрежи. DoS нападот се случува кога противник предизвикува мрежата да стане недостапна за легитимните корисници, или услугите да бидат прекинати или одложени. Овој напад може да ги исклучи сите комуникации во дадена област. DoS нападите на безжичните мрежи навистина е тешко да се детектираат и спречат. Предмет на овој труд е да се разгледаат DoS нападите кај безжичните мрежи, да се опишат некои од методите кои се користат за намалување на ефектите од овие напади и да се изврши анализа на ефикасноста на различните методи на одбрана од напади, во случајов одложување на деавтентикациското барање и автентикацискиот механизам со случајни битови.*

Клучни зборови *– DoS, напад, напаѓач, безжична мрежа, IEEE 802.11*

1. ВОВЕД

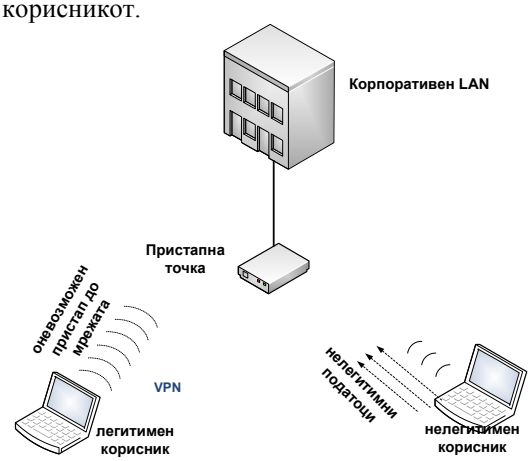
Во борбата за што поголема флексибилност и продуктивност на компаниите и организациите, огромна е побарувачката на безжичните решенија. Целта за одржување на ефикасноста и конкурентската предност во голема мера зависи и од користењето на безжичните мрежи. Една од главните придобивки на користењето на безжичните решенија е мобилноста која ја нудат. Секако, големо е значењето и на заштедата на трошоците во споредба со традиционалната инсталација на жичните мрежи. Сепак, една многу важна работа која треба да ја спроведат организациите е зголемување на контролата и сигурноста на безжичната мрежа од напади. Безжичните мрежи се многу ранливи на DoS (Denial of Service) и на DDoS (Distributed Denial of Service) нападите и резултат на овие напади може да биде од деградација на мрежата, па се до целосна загуба на достапноста на безжичната мрежа [1]. Земајќи во предвид дека повеќето безжични технологии користат нелиценцирани фреквенции, повеќе од јасно е дека поради тоа е зголемена можноста за интерференција од различни електронски уреди. За да се избегнат последиците од ваквите напади, кои може да бидат фатални за нападнатиот систем, од огромно значење е детекцијата, превенцијата и ублажувањето на ефектите од истите. Причините за ваквите напади може да бидат од различна природа: некогаш се изведуваат од злоба и од забава, но некогаш се изведуваат од конкурентни и политички цели. Најголем и најпознат напад што се случил досега од политички побуди, е нападот врз Естонија. DDoS нападите се случија на 27 Април, 2007 година и ги "осакатија" web-страните на Парламентот на Естонија, Премиерот, банките и многу други владини агенции. Аналитичарите кои го анализираа нападот пронајдоа траги на web-страните и наведуваат дека во нападите биле вклучени руски хакери. Сепак, анализата на злонамерниот сообраќај покажува дека во нападите биле користени компјутери од САД, Канада, Бразил, Виетнам и други земји, што е и најкарактеристично за ваквиот тип на напади [2].

2. DoS И DDoS НАПАДИ

Целта на секој DoS и DDoS напад е да се спречи пристапот на корисниците до мрежните ресурси, т.е., да им се одбие бараната услуга. DoS напад е кој било настан што ги намалува или елиминира капацитетите на безжичната мрежа при извршување на своите функции. На повеќето DoS напади целта е мрежниот опсег на хостот или линиските ресурси на компјутерската врска. Значи, мрежниот систем е полн со сообраќај или барања за остварување на конекција.

DoS нападите се однесуваат на достапноста (обезбедување на овластените лица да имаат пристап до податоци, услуги или други компјутерски и мрежни ресурси), така што ја спречуваат комуникацијата меѓу мрежните уреди или спречуваат еден единствен уред да учествува во сообраќајот. Попречувањето (jamming) се случува кога со намерна или ненамерна интерференција се "потиснува" комуникацискиот линк на испраќачот или примателот, со што се намалува ефикасноста на линкот, па линкот може да стане дури и бескорисен. Причина за ваквото попречување на целата мрежа може да биде DoS нападот. Целата област, вклучувајќи ги и базната станица и клиентот, се преплавени, така што нема станици што можат да комуницираат едни со други. Овој напад ги затвора сите комуникации во дадената област [3]. Доколку се применува на пошироко поле, овој тип на напад може да бара значително количество на електрична енергија.

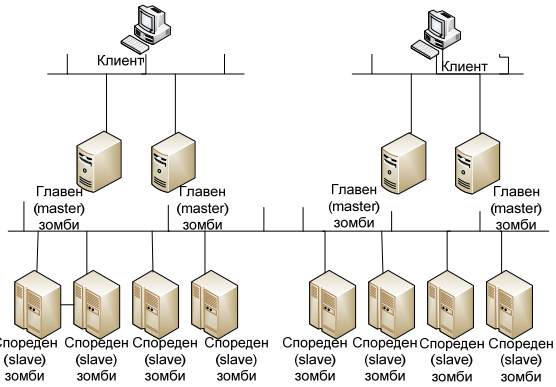
Во безжичната мрежа која од безбедносна гледна точка се потпира исклучиво на IPSec, пристапната точка мора да биде мост до целиот сообраќај кон жичната мрежа. Ова им овозможува на корисниците да автентицираат и воспоставуваат IPSec конекција, но исто така, им овозможува на злонамерните корисници да испратат рамки кон пристапната точка. Така, напаѓачот може да ја поплави пристапната точка со податоци, прекинувајќи ја легитимната конекција на корисникот.



Сл. 1 – Напад со одбивање на услуга (DoS)

Друг пример на DoS напад би можел да биде кога напаѓачот ја снима претходната дисконектирачка порака и повторно ја препраќа, што резултира со губење на конекцијата на легитимниот корисник со безжичната мрежа [4].

За разлика од обичните DoS напади, дистрибуираните DoS напади (DDoS) се посериозна закана и се однесуваат на симултано и координирано напаѓање на одреден број на хостови, над одредена цел. Компромитирајќи повеќе хостови во исто време, се спречуваат корисниците од користење на услуга. Овие напади вообичаено се применуваат кога има повеќе извори, кои се шират низ целата мрежа. Нападнатиот мрежен систем е преоптоварен од лажни барања за услуги, па затоа ја одбива услугата. Кај овој дистрибуиран напад, за разлика од единствениот напаѓач кај DoS нападот, потешко е да се утврди кој е напаѓачот. Кај DDoS нападите може да има 100 или повеќе различни напаѓачи (мрежни системи) кои напаѓаат еден мрежен систем, додека најпознатите и најчестите DDoS напади користат и повеќе од илјадници вакви системи. Компромитирачките мрежни системи се избираат случајно, а колку е поголем нивниот број, толку е помоќен DDoS нападот. Често ваквиот напад вклучува две нивоа на зомби машини: главни (master) и споредни (slave) зомби. Напаѓачот ги координира и повикува главните зомби, кои пак ги координираат и повикуваат спородните.

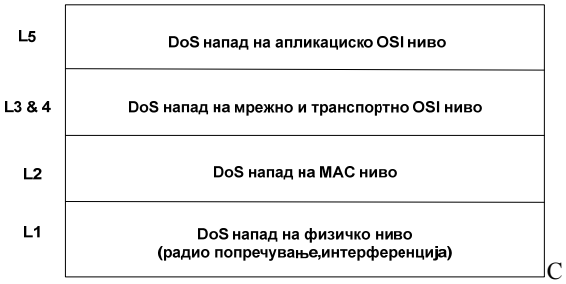


Сл.2 – Напад со Дистрибуирано Одбивање на Услуга (DDoS)

Потоа компромитираните мрежни системи се координираат од далечина за да се изврши нападот. Вообичаено, овие напади предизвикуваат толку многу дополнителен мрежен сообраќај, што претставува тешкотија за легитимниот сообраќај да стигне до легитимните мрежни уреди. Сообраќајот може да дојде од валидна IP адреса или од случајна адреса креирана од slave процесите. Ако системот е ранлив на напад извршен од страна на спородниот (slave) процес, тој ќе падне и ќе паѓа при секој нареден обид да се поврати. Дури и ако системот не е дефектен, неговата мрежна конекција ќе биде заситена.

3. КЛАСИФИКАЦИЈА НА DoS НАПАДИТЕ

DoS нападите може да бидат насочени кон различните слоеви од OSI референтниот модел на мрежата, а одбивањето на нападите има за цел да ги изолира мрежните ресурси од оние кои ги загрозуваат.



Сл. 3 – Класификација на DoS напади

DoS нападот на апликациско OSI ниво се врши со испраќање на голем број барања кон апликацијата, во однос на бројот за кој таа е димензионирана. На ова ниво не постои разлика помеѓу DoS нападите во жична и во безжична мрежа [1]. Напаѓачот се обидува да ја искористи слабоста на апликациските протоколи како DNS, HTTP или испраќа злонамерен код во форма на вирус, црв или тројански коњ, кој потоа развива штетен ефект врз засегнатиот уред [5]. Серверот обично се обидува да ги исполни барањата на корисникот, но и да ги одржи услугите во живот.

Во еден момент на DoS нападот, серверот не може да одговори на сите барања, па одбива да ја изврши услугата. DoS нападите на апликациско ниво се присутни подолго време и поради тоа развиени се многу ефективни сретства за заштита на уредите од ваквите напади (протоколни стекови, автентикација, firewall-и).

DoS нападот на мрежно и транспортно OSI ниво се однесува на барања за воспоставување на врска кон хостот и онеспособување на ова ниво со испраќање на голема количина на податоци на мрежата. Ако мрежата дозволува на било кој клиент да се асоцира, таа станува ранлива на напади на мрежно ниво. Кај 802.11 мрежите кои користат заеднички медиум, напаѓачот може да ја поплави мрежата со сообраќај и така да го оневозможи пристапот кон другите уреди поврзани на дадена AP [6]. И на ова ниво, како и на апликациското, не постои разлика помеѓу DoS нападите на жична и на безжична мрежа и токму затоа може да се искористат предностите на достапноста на широкиот спектар на решенија против ваквите напади [1]. Можни напади се ping-of-death (специјално креирани ping пакети чија цел е уништување на уредот кој ги добива), land attack или напад од земја (TCP SYN сегмент со фалсификувана изворна IP адреса која предизвикува ACK војна кај примачот со дестинациска IP адреса), smurf (поплава од ping пакети) и TCP SYN flood (преплавување на примачот со SYN сегменти, така што секој сегмент завзема нова податочна структура за нова конекција) [5]. Бидејќи овие напади се добро проучени и разбрани, постојат повеќе решенија, како што се: филтрирање на пакети, мрежни стекови, детектирање на упад, обликување на сообраќајот и ACL (листи за контрола на пристап).

Главната разлика меѓу нападот на жична и нападот на безжична мрежа се манифестира кај физичкото и кај MAC нивото на OSI референтниот модел.

Нападите на MAC (Контрола на Пристап кон Медиум) нивото [5] се многу лесни за монтирање. Овој вид на напад ги користи слабостите на безжичниот протокол и не може да се отстрани со додавање дополнителен уред или нов софтвер, се додека самиот протокол не се модифицира за да може да ги спречи идните напади. Безжичните мрежи се особено ранливи на напади на ова ниво, бидејќи користат заеднички медиум и на тој начин напаѓачот доаѓа лесно и брзо до информации за мрежните учесници. Мрежниот администратор не може многу да стори против експлоатирањето на протоколот. Неговите активности се насочени кон следење на сомнителните активности и обид за изолирање на нападнатите уреди и вадење од употреба.

DoS нападите на физичко OSI ниво, кога се работи за безжични мрежи, предизвикуваат големо внимание. Очигледно е дека попречувањето со шум-сигнали во безжичните мрежи, познато како **RF напад**, може да го намали капацитетот на мрежата до неприфатливо ниво. Намерната или ненамерната интерференција со други радио предаватели е уште една можност за загушување на перформансите на безжичната мрежа [7]. Спротиставувањето на безбедносните закани на физичко ниво е многу тешко. Всушност, многу малку може да се направи против нападите на ова ниво, освен засолнување од електромагнетните зрачења и користење на некои алатки за идентификување на напаѓачот и ако е можно, негово изолирање. Среќна околност е тоа што, поради губењето на моќта на сигналот при удвојување на растојанието помеѓу испраќачот и примачот, овие напади се потешки за извршување. Ова значи дека нивото на јачината на сигналот брзо ќе се намали со порастот на растојанието, а тоа пак значи дека за да биде реална закана, напаѓачот треба да биде блиску до целта која ја напаѓа или да ја зголеми моќта на пренесување на сигналот [5].

4. DoS НАПАДИ КАЈ 802.11 МРЕЖИТЕ

802.11 стандардот припаѓа на фамилијата IEEE стандарди, кои го дефинираат MAC и физичкото ниво во безжичната комуникација помеѓу клиентите и базните станици. Генерално, се состои од безжични клиенти кои комуницираат со AP (пристапна точка) [8].

Постојат два главни типови на DoS напади кај 802.11 мрежите: *RF напади* и *напади врз 802.11 протоколот*.
RF нападите настануваат на физичкото ниво на OSI референтниот модел и се познати и како напади со попречување, а кратко се опишани во Поглавје 3.
Нападите врз 802.11 протоколот се однесуваат на второто (MAC) ниво. Овие напади ги користат слабостите на идентитетот и слабостите на MAC.[8]

4.1. Слабости на идентитетот

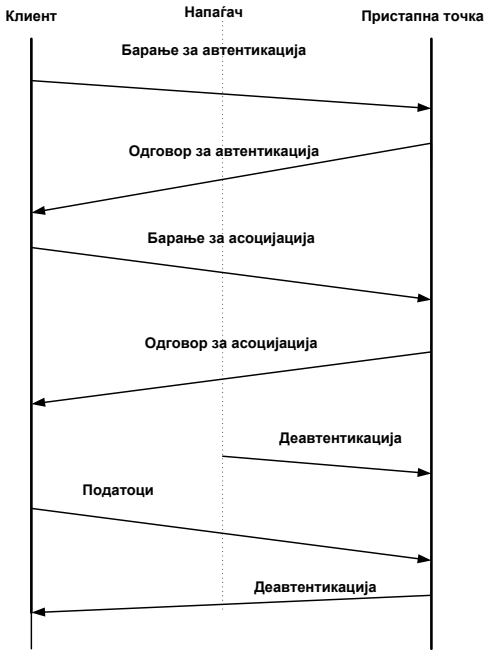
Јазлите кај 802.11 стандардот, исто како и јазлите кај жичните мрежи, се идентификуваат со уникатна MAC адреса. Рамките не се автентицирани, што значи дека напаѓачот може да ја промени својата MAC адреса и да ги измами останатите јазли, при што може да се предизвикаат следните три видови на напади:

- Деавтентикациски напад (најефективен)
- Дисасоцијациски напад
- Напад на режимот за заштеда на моќност

Деавтентикациски напад:

Најпрво клиентот треба да изврши постапка на автентицирање кон селектираната AP со својата MAC адреса. Дел од автентикацискатa рамка е

порака која овозможува клиентот експлицитно да се деавтентицира од АР. Токму тоа е слабоста која ја користи напаѓачот. Имено, ова се реализира на тој начин што може да се испрати лажна деавтентикациска порака, која ќе ја суспендира комуникацијата помеѓу клиентот и АР, што значи предизвикан е DoS напад [5]. Резултат е тоа што клиентот ќе мора да ја обнови комуникацијата со АР, така што повторно ќе треба да се автентицира.



Сл. 4 – Деавтентикациски напад

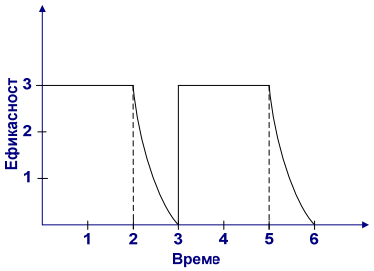
Со повторување на нападот, клиентот е изолиран од пренос и прием на податоци на неодредено време. Нападот може да се извршува врз индивидуален клиент или врз сите клиенти. При напад врз индивидуален клиент, напаѓачот ја користи адресата на клиентот, кажувајќи и на АР да го деавтентицира тој клиент. При напад врз сите клиенти, напаѓачот ја користи АР кажувајќи им на сите клиенти да се деавтентицираат.

Дисасоцијациски напад:

По автентикацијата клиентот мора да се поврзе со АР за да и овозможи на АР да ги препраќа пакетите кон клиентска страна. Како и при деавтентикација, 802.11 обезбедува барања за дисасоцијација, кои ќе и кажат на АР да го запре сообраќајот кон клиентот. Идентично на деавтентикацискиот напад и тука напаѓачот испраќа лажна дисасоцијациска порака предизвикувајќи АР да се дисасоцира од клиентот, што резултира во DoS напад. За обновување на комуникацијата, потребно е клиентот повторно да се реасоцира кон АР.

Споредба на ефикасноста на деавтентикацискиот и дисасоцијацискиот напад:

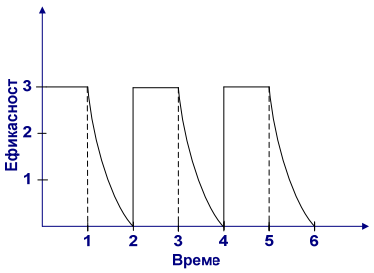
Во следните неколку реченици ќе ја објасниме ефикасноста на овие два напади Најпрвин го објаснуваме деавтентикацискиот напад. Бидејќи автентикацијата се случува пред асоцијацијата, за опоравување од овој напад потребни се две постапки, прво реавтентикација, а потоа реасоцијација. Значи функцијата на нападот до извршувањето на втората постапка го има највисокото ниво на ефикасност. По реасоцијацијата има пад на функцијата. Во следниот момент кога има нов напад, ефикасноста на нападот повторно го достигнува највисокото ниво и тоа е така се до постапката на реасоцијација. Графичкиот приказ на два последователни деавтентикациски напади е следниот:



Сл. 5 – Графички приказ на два последователни деавтентикациски DoS напади

Од графикот се гледа следното: се случува деавтентикациски напад. Во моментот 1 од временската оска се врши реавтентикација, во моментот 2 се врши реасоцијација, па ефикасноста на нападот паѓа, за да во следниот момент 3, кога се случува нов напад, ја достигне повторно максималната вредност. Постапката се повторува. Значи во моментот 4 имаме реавтентикација, во моментот 5 реасоцијација и повторен пад на ефикасноста.

Кога имаме дисасоцијациски DoS напад потребна е само една постапка за опоравување од нападот, а тоа е реасоцијација. Значи функцијата ќе го има највисокото ниво на ефикасност до случувањето на постапката реасоцијација, кога ќе има пад и повторно ќе има подем во следнот момент на случување на напад. Графички ова би изгледало како на Сликата 6.



Сл. 6 – Графички приказ на три последователни дисасоцијациски DoS напади

Графички се прикажани три последователни дисасоцијациски напади. Значи се случува напад, а во моментот 1 се врши постапка на реасоцијација, па видлив е падот на ефикасноста од нападот. Во моментот 2 има повторно напад и

максимално ниво на ефикасноста од нападот, а во моментот 3 повторно има реасоцијација. Следен напад во моментот 4 и пак највисоко ниво на ефикасноста, за да во следниот 5-ти момент при реасоцијацијата се случи повторно пад на функцијата.

Со анализа и споредба на овие два графици го утврдивме следното:

И во двата случаи на напади, земено е времето да биде исто, до 6-тата единица од временската оска. Исто така, претпоставуваме дека следниот напад се случува во следната временска единица. При деавтентикациски напад функцијата го има својот максимум во времетраење од 4 мерни единици. При дисасоцијациски напад, пак, функцијата го има својот максимум во времетраење од 3 мерни единици. Значи, деавтентикацискиот напад, споредено со дисасоцијацискиот напад е максимално ефикасен подолго време, во ист временски интервал. Исто така, во првиот случај на деавтентикациски напад, имаме два пати пад на функцијата, а во случајот кај дисасоцијацискиот напад има 3 пати пад на функцијата, што исто така е показател при анализата на ефикасноста на овие два напади. Од претходно изнесеното може да се утврди дека деавтентикацискиот напад, споредено со дисасоцијацискиот, е поефективен.

Напад на режимот за заштеда на моќност:

Поради заштеда на енергијата, на клиентите им е дозволено да влезат во т.н. состојба на сон (sleep) и во оваа состојба AP ги баферира пакетите наменети за клиентите. Клиентите повремено се будат и ја анкетираат AP за баферираните пораки. AP пак, повремено испраќа TIM (Traffic information map) пакети, за да го извести клиентот за баферираните податоци. Слабост е тоа што напаѓачот може да лажира анкета или TIM пораки, што резултира во три видови на напади:

- Напаѓачот може да предизвика анкетна порака, што ќе предизвика AP да ги отфрли пакетите додека клиентот „спие“.
- Напаѓачот може да лажира TIM пораки, уверувајќи го клиентот дека не постојат баферирани податоци.
- Напаѓачот може да фалсификува клучна (важна) синхронизирачка информација како што е TIM периодот, оневозможувајќи му на клиентот да се синхронизира со пристапната точка.

Во споредба со останатите напади, овие напади се потешки за извршување, поради firmware ограничувањата. За разлика од деавтентикацискиот напад, може да се констатира дека нападот на режимот за заштеда на моќност е понеефикасен.

4.2. Слабости на MAC

MAC нивото го контролира пристапот на клиентот кон медиумот, овозможувајќи брз пренос ослободен од колизија. За превенција од колизии се користи комбинација од механизми за физичко откривање на носител и виртуелно откривање на носител . Физичкото откривање на носител користи CSMA/CA со временски прозорци (Time windows). Виртуелното откривање на носител пак, користи RTS/CTS со NAV.

Физичко откривање на носител

CSMA/CA е скратеница за Carrier Sense Multiple Access with Collision Avoidance (Повеќестепен Пристап со Откривање на Носител со Избегнување на Колизија). Работи како жичниот Ethernet, освен што користи Избегнување на колизија наместо Детектирање на колизија. Покрај тоа, за да се даде приоритетен пристап до медиумот, користи временски прозорци (Time windows). Пред испраќањето на податоците, клиентите мора да го набљудуваат тивкиот медиум за еден од временските прозорци. Двата најважни временски прозорци се краткиот простор помеѓу рамки (SIFS) и просторот помеѓу рамки со дистрибуирана функција за координирање (DIFS).

DIFS го дефинира времето во кое медиумот мора да биде слободен пред клиентот да може да пренесува. SIFS го дефинира времето на чекање за пренос, откако претходната рамка е испратена. За разлика од DIFS ова е пократко време. За да се избегнат пренесувањата на сите јазли веднаш по истекувањето на DIFS, времето по DIFS е поделено на слотови. Секој клиент избира временски слот во кој ќе пренесува, а доколку дојде до колизија, се користи случаен backoff алгоритам пред следното препраќање.

Напад врз временските прозорци:

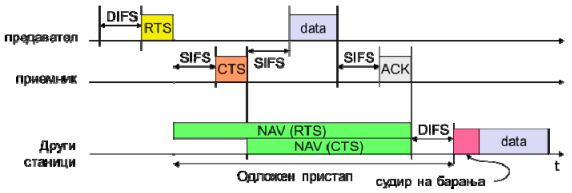
Секој клиент кој пренесува, мора да почека најмалку еден SIFS интервал, а можеби и подолго. Напаѓачот може целосно да го монополизира каналот со испраќање на сигнал пред да заврши секој SIFS интервал. Овој напад е ограничен.

Виртуелно откривање на носител

За спречување на колизија помеѓу два клиенти кои не се слушаат помеѓу себе, потребен е некаков механизам. Кога еден клиент сака да пренесува пакет, прво испраќа RTS (барање за испраќање). Во RTS се вклучени информации за изворот, дестинацијата и времетраењето. Клиентот на ова одговара со CTS (слободно за испраќање) порака.

Сл. 7 – MAC податочна рамка

Во MAC податочната рамка има поле "Времетраење", кое содржи број даден во μs, во кои каналот е зафатен. "Времетраење" полето се користи во размената на RTS/CTS секвентни пакети.



Сл. 8 – Трансакција помеѓу две станици и NAV сетирање на соседите

Сите клиенти при добивањето или на RTS и/или на CTS, ќе ги сетираат своите индикатори за Виртуелно откривање на носител наречени Network Allocation Vector (NAV). Клиентите, кога ќе го „слушаат" медиумот, ќе ги користат овие информации заедно со Физичкото откривање на носител. Само кога вредноста на NAV на клиентот ќе достигне 0, е дозволено пренесување преку медиумот.

Напад врз NAV:

Овој напад произлегува од фалсификување на "Времетраење" полето на MAC пакетот. Напаѓачот може да го постави ова поле да има високи вредности, па така ќе предизвика NAV вредностите да бидат зголемувани, а за другите ќе го спречи пристапот кон каналот. Максималната вредност може да биде 32767, што е околу 32ms. Напаѓачот е потребно да пренесува само 30 пати во секунда. Нападот е подобрен ако времетраењето на RTS се фалсификува, па така клиентите ќе пропагираат напад со CTS.

5. МЕТОДИ ЗА НАМАЛУВАЊЕ НА ЕФЕКТИТЕ ОД DoS

Кога станува збор за одбрана од DoS напади на физичко ниво кај безжични мрежи, нема многу нешта што би можеле да се направат, освен поставување на хардверска заштита која би ги спречила ефектите од DoS нападите. Најдобар начин е да се задржат радио брановите внатре и да останат неоштетени со користење на антени кои ќе ги пренасочуваат сигналите. Исто така, постојат и некои RF заштитни материјали кои може да се постават на ѕидовите и на прозорите на зградите, но тие се прилично скапи. Ако не е можно поставување на ваква заштита, тогаш најдобра алтернатива е да се изолираат напаѓачите колку е можно подалеку од безжичниот систем [9].

Во случај напаѓачката станица да е опремена со предавател со тесен опсег, тогаш многу ефективен метод во борбата против попречувачките акции може да биде *брзото фреквентно потскокнување* [10]. Експериментално е покажано дека попречувачките напади од една станица се релативно неефективни против акцијата од брзите фреквентни потскокнувања на легитимните корисници. Ако бројот на напаѓачки станици се зголемува, тогаш ефективноста на брзото фреквентно потскокнување значително се намалува, се додека сите канали не бидат попречени од страна на најмалку една напаѓачка станица. Имплементирањето на брзото фреквентно потскокнување носи некои дополнителни проактивни користења на методи за превенција и не е многу ефикасно, ако не е детектирано постоење на DoS напад.

Кај нападите од MAC нивото постојат повеќе видови на механизми и методи за одбрана, кои зависат од тоа кој напад е извршен. Во делот кој следува, опишани се неколку методи и механизми кои се однесуваат на деавтентикациските и дисасоцијациските напади. Еден метод кој се однесува на деавтентикацискиот напад е со *автентикација на управувачките рамки* [8]. Овој метод се покажал како не многу ефикасен, поради тоа што не е изводливо користење на софтвер кој ќе се надгради, а проверката на стандардната рамка побарува многу време. Поефикасен метод е *одложување на деавтентикациското барање* [8]. Се базира на набљудуваното однесување на легитимните клиенти кои не се деавтентицираат, па испраќаат податоци. Интервалите на одложување се мали и се во траење 5-10 секунди. Барањето се реализира ако нема други рамки кои се примени од изворот. Постапката е следна: AP, по примањето на деавтентикациското барање, го сместува барањето во редица на чекање за определен временски период. Ако времето измине и ако нема реализација на сообраќај од тој јазол, тогаш барањето е прифатено и јазолот е деавтентициран. Од друга страна, ако сепак има реализирање на сообраќај од тој јазол уште пред да помине определениот временски период, тогаш деавтентикациското барање не е прифатено [11].
Уште еден метод на заштита при овие напади е со *криптографска заштита на управувачките рамки.* Овој метод е предмет на 802.11w стандардот, кој е промовиран во Ноември, 2009 година, од страна на IEEE [10].
Еден од механизмите за заштита на 802.11 мрежите од деавтентикациски и дисасоцијациски напад е *автентикациски механизам со случајни битови* [12]. Овој механизам на одбрана од DoS напади, може да искористи максимум 13 бита за заштита на операциите на автентикациските/ асоцијациските процедури. Контролното поле од рамката би можело да донира 2 бита, а телото на рамката би можело да допринесе со најмногу 11

бита. Се претпоставува дека клучот за размена е споделен помеѓу двата јазли кои комуницираат. Разменетиот клуч ќе се користи за да генерира сесија на клучеви што може да се користат за да генерираат заеднички случаен bitstream. Исто така, алгоритмот е јавен, а клучот кој се користи е таен. Јазлите во истиот основен сет на услуги (BSS) го користат заедничкиот сесиски клуч и алгоритам за независно да генерираат идентичен, случаен проток на битови (bitstream). Протокот е поделен на еднакви делови и секој од нив има "N" битови за проверка и се нарекува "N случен бит". На секој дел му е доделен број на индекс. Кога јазол (AP или STA) испраќа (де)автентикациски или (дис)асоцијациски рамки, ја вметнува моменталната 3-битна единица во неискористените позиции на битовите на секоја рамка, а потоа го поместува индексот да покажува на наредната единица. Јазолот-примач треба да пронајде дека случајниот бит за проверка во примената рамка одговара на соодветната bitstream единица на примачот; во спротивно рамката ќе биде одбиена. Ако напаѓачот ги монтира деавтентикациските или дисасоцијациските напади со поплавување, потребно е да се заменат деавтентикациските или дисасоцијациските напади, соодветно. Меѓутоа бидејќи напаѓачот не ги знае вредностите за одредени позиции мора да користи некој метод за проверување на битовите, се додека не се совпаднат. Една опција на напаѓачот е да користи "brute-force" пристап за да ги помине сите можни вредности на случајните битови. Една од лажните деавтентикациски/ дисасоцијациски рамки ќе го помине тестот за автентикација. Стапката на успешност на напаѓачот за да ја дисконектира сесијата помеѓу AP и STA е обратно пропорционална со бројот на деавтентикациските/ дисасоцијациските лажни рамки. Ако бројот на битовите за проверка се зголеми, стапката на успех за постигнување (овозможување) на DoS напад се намалува експоненцијално.

Што се однесува до одбраната од нападите врз NAV, еден вид на одбрана се базира на фактот што легитимната вредност на "Времетраење" полето е релативно мала [8]. Се поставува означувач на максималната вредност од времетраењето на добиените рамки. Ако станицата прими рамки со времетраење поголемо од означената вредност, се скратува времетраењето на означената вредност. Овој метод бара стриктно придржување кон ниската и високата означена вредност. Ниската означена вредност е еднаква на износот на времето потребно за да се испрати ACK. Високата означена вредност се користи кога податочниот пакет ја следи набљудуваната рамка.

6. ИСТРАЖУВАЊЕ И АНАЛИЗА

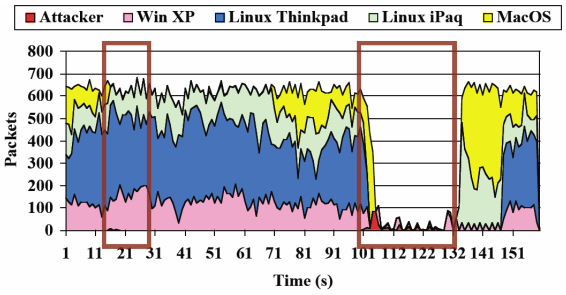
Истражувањето кое го направивме се однесува на споредба на ефикасноста на двата претходно опишани механизми за заштита од деавтентикациски напад. Тоа се *методот на одложување на деавтентикациското барање* и *автентикацискиот механизам со случајни битови*. За анализа на овие два методи ги искористивме експериментите изведени во наведените референци [8] и [12].

Експериментот на методот со одложување на деавтентокациското барање [8] се состои во следното: тестирана е мала 802.11 мрежа составена од 7 машини: 1 напаѓач (iPAQ H3600 со Dlink DWL-650), 1 пристапна точка (со Linux HostAP драјвер), 1 набљудувачка станица (ги снима резултатите од тестот) и 4 легитимни клиенти (winXp, Linux Thinkpad, Linux iPAQ, MacOS X).

Сценариото е дека секој од клиентите се обидува, преку ftp да пренесе голема датотека кон пристапната точка. Се случуваат 2 напади, едниот е напад врз индивидуален клиент (MacOS X), во 15-тата секунда со времетраење од 8 секунди и вториот е напад врз сите клиенти, кој се случува во 101-вата секунда и трае 26 секунди.

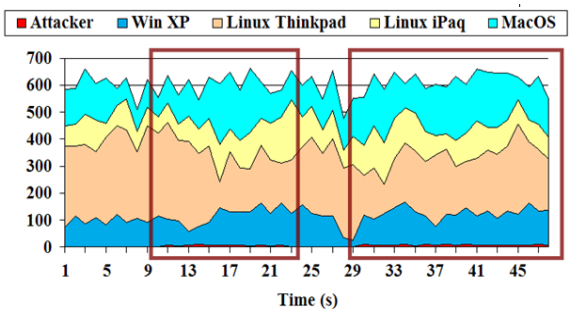
Во случај кога не се користи одбранбен механизам од DoS напад, иако првиот напад трае помалку од 10 секунди, клиентот не може да пренесува пакети околу 1 минута. Периодот на опоравување, во кој клиентот бара други пристапни точки, е околу 50 секунди. Вториот напад трае подолго, а од добиените резултати кои се гледаат на Слика 9, може да се утврди дека времето на опоравување е различно кај различните клиенти, но за сите да се опорават од нападот, потребни се 19 секунди.

За да се истестира оваа одбрана, модифицирана е AP која во експериментите се користи како што е претходно опишано, користејќи timeout вредност од 10 секунди за секое управувачко барање.



Сл. 9 – Деавтентикациски напад кога не се користи одбранбен механизам

. Повторно се извршува претходниот експеримент. Резултатот може да се види на Слика 10, при што е тешко да се каже дека нападот е активен и клиентските јазли ја продолжуваат својата активност.



Сл. 10 – Деавтентикациски напад кога се користи одбранбен механизам

Вториот експеримент [12] се однесува на автентикацискиот механизам со случајни битови. Користени се 4 лаптопи со карактеристики дадени во следната табела:

Функција	Модел на лаптоп	CPU	RAM	802.11 PC Card Model	Оперативен систем	PC Card driver & софтвер
Домаќин Пристапна точка	HP Compaq Nc 6230	Intel P.M 1.73 GHz	1.00GB	Netgear 802.11b MA401 (Chipset:Prism2)	LinuxFC3 Kernel: 2.6.9-1.667	Домаќин АР драјвер со Master режим
Станица (STA)	Asus A2500H	Intel P4 2.8 GHz	224MB	Intersil Prism 2.5 802.11b PC card	LinuxFC3 Kernel: 2.6.9-1.667	Домаќин АР драјвер со Management режим
Напаѓач	HP Compaq Nc 6230	Intel P4 1.73GHz	1.00GB	Netgear 802.11b MA 401 (Chipset:Prism2)	LinuxFC3 Kernel: 2.6.9-1.667	Домаќин АР драјвер со void 11
Монитор	Toshiba TE2100	Intel P4-M 1.80GHz	256MB	Asus WL-100 (Chipset:Prism2)	LinuxFC3 Kernel: 2.6.9-1.667	Домаќин АР драјвер Kismet Ethreal

Табела.1 – Деавтентикациски напад кога се користи одбранбен механизам

Сценариото е следно: напаѓач монтира деавтентикациски напад. Тој не ги знае вредностите за одредени позиции и мора да користи некој метод за проверување на битовите, се додека не се совпаднат. Една опција на напаѓачот е да користи "brute-force" пристап за да ги помине сите можни вредности на случајните битови.

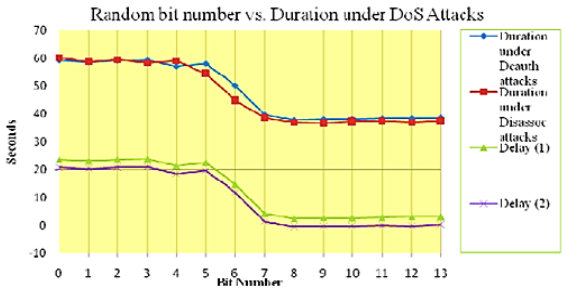
Процедурата на тестирање на експериментот е опишана на следниов начин и се повторува барем 10 пати:

(а) Како основен модел се користени нормални FTP сесии.

(б) Симулиран е перфектен одбранбен механизам со игнорирање на сите деавтентикациски и дисасоцијациски рамки примени од страна на пристапната точка. Ова е за да се определи чист overhead предизвикан од постоењето на нападите со поплавување.

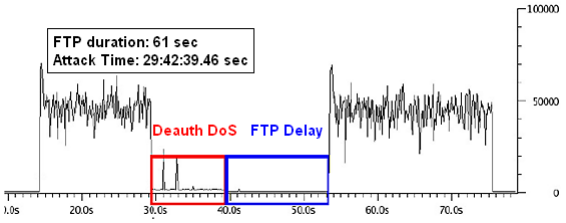
(в) Ефикасноста на механизамот за случајна проверка е утврдена од просечното времетраење на пренос на датотека во однос на бројот на случајни битови кои се користат. Бројот на тестирани случајни битови се движи 0-9.

Со тестирањето се добиени следните резултати:



Сл. 11 – Заштита обезбедена со различен број на случајни битови

Од горниот график се гледа дека колку повеќе случајни битови се користат, толку се помали ефектите од деавтентикацискиот и дисасоцијацискиот напад. Ако N=5, не е доволно за одбрана од овој напад. Напаѓачот може да испраќа 80 лажни деавтентикациски и дисасоцијациски рамки во секунда. Така, напаѓачот добива 80/32=2.5 успешни обиди. Ако бројот на битови се зголеми на 7, бројот на успешни обиди ќе се намалат на помалку од 1.



Сл. 12 – Незаштитена ftp сесија при деавтентикациски напад

На Слика 12 прикажано е дека ftp сесијата не се опоравува веднаш после стопирањето на нападот, туку после 13 секунди.

Експериментот се врши над датотеки со различна големина и со различен број на случајни битови. Резултатите се прикажани на следната табела. За секоја комбинација на датотека и број на случајни битови, преносот на датотеката е иницираан 10 пати во 10 секунди за време на континуиран деавтентикациски напад.

Големина на датотека	Број на случајни битови													
	0	1	2	3	4	5	6	7	8	9	10	11	12	13
1к	23.7	23.6	23.6	23.8	22.5	20.6	15.3	2.5	2.5	2.7	2.7	2.9	3.1	3.0
2к	23.6	23.4	23.8	23.5	22.7	22.5	14.5	2.7	2.6	2.8	2.9	3.0	2.9	3.1
4к	23.5	23.7	23.5	23.6	22.5	22.3	14.9	2.6	2.6	2.7	2.8	2.8	3.0	3.0
8к	23.6	23.6	23.5	23.7	22.4	20.5	14.7	2.8	2.7	2.7	3.0	3.1	2.9	2.9
64к	23.7	23.6	23.7	23.6	22.7	22.5	15.1	2.7	2.5	2.8	2.7	2.9	2.8	3.2
512к	23.6	23.5	23.6	23.7	22.1	22.0	14.6	2.5	2.7	2.6	2.9	2.8	2.9	2.8
1М	23.7	23.5	23.6	23.8	21.9	22.3	14.8	2.8	2.7	2.5	2.8	2.9	2.9	3.0
2М	23.7	23.7	23.5	23.6	22.5	22.5	15.2	3.1	2.8	2.8	2.7	2.9	3.1	3.0
4М	23.6	23.6	23.7	23.7	22.6	22.4	14.7	2.6	2.7	2.6	2.7	3.1	3.0	3.1
8М	23.5	23.7	23.5	23.8	22.5	22.3	14.6	3.9	2.6	2.7	2.9	2.8	2.9	3.0
16М	23.7	23.6	23.6	23.5	22.7	22.3	14.5	4.2	2.8	2.7	2.8	2.9	2.9	3.1
32М	23.7	23.7	23.6	23.8	22.3	22.2	14.6	2.5	2.6	2.6	3.0	2.9	3.1	2.9

Табела.2 – FTP доцнење на пренос предизвикано од деавтентикациски напади

Врз основа на овие експериментални резултати, заклучокот е дека доцнењето на преносот не зависи од големината на датотеката, туку од бројот на случајни битови кои се користат.

Нашата анализа се однесува на претходно опишаните методи, и тоа кога е поефикасен првиот, а кога вториот метод.

Прво заклучуваме дека кај првиот метод, ефикасноста на одбраната ќе зависи во голема мерка од тоа после колку време по испраќањето на напаѓачката деавтентикациска рамка клиентот ќе испрати податоци кон пристапната точка. Ако тоа време е помало од 10 секунди, колку што е времето на интервалот на одложување, тогаш пристапната точка нема да ја прекине врската со клиентот и ќе имаме ефикасна одбрана од нападот. Ако пак тоа време е поголемо од 10 секунди, на пример ако клиентот податоците ги испрати после 13 секунди, тогаш пристапната точка по истекот од 10 секунди предвидени за интервалот на одложување ќе го потврди дисконектирањето со клиентот и пакетите кои се испратени од клиентот нема да стигнат до посакуваната дестинација. Во овој случај нема ефикасна одбрана од нападот.

Кај вториот метод пак, со експериментот е покажано дека ефикасноста на нападот не зависи од големината на датотеката која се пренесува туку само од бројот на случајни битови. Така, ефикасноста на одбраната е мала ако бројот на битови е помал од 6, за 6 бита веќе имаме поголема ефикасност, а најголема ефикасност има ако бројот на битови е 7 и повеќе.

Правиме споредба на 4 случаи и тоа:

1. При метод на одложена деавтентикација со интервал на одложување од 10сек, при што клиентот праќа податоци после 8сек од почетокот на деавтентикациските барања, резултат би бил продолжување на врската (нема прекин). При метод на автентикација со случајни битови, кога бројот на битови е 5, се случуваат 2.5 успешни напади во секунда и време на оправување од 22 секунди (според експериментот).

   Во овој случај методот на одложена деавтентикација е поефикасна одбрана отколку методот на автентикација со случајни битови.

2. При метод на одложена деавтентикација со интервал на одложување од 10сек, при што клиентот праќа податоци после 8сек од почетокот на деавтентикациските барања, резултат би бил продолжување на врската (нема прекин). При метод на автентикација со случајни битови, кога бројот на битови е 7, се случуваат 0.625 успешни напади во секунда и просечно време на оправување од 2.9 секунди (според експериментот).

   И во овој случај методот на одложена деавтентикација е поефикасна одбрана отколку методот на автентикација со случајни битови.

3. При метод на одложена деавтентикација со интервал на одложување од 10сек, при што клиентот праќа податоци во 13-тата секунда од почетокот на деавтентикациските барања, резултат е прекин на врската и време на оправување од 21 секунда (според експериментот со напад над сите клиенти). При метод на автентикација со случајни битови, кога бројот на битови е 5, се случуваат 2.5 успешни напади во секунда и време на оправување од 22 секунди (според експериментот).

   И во ваков случај методот на одложена деавтентикација е поефикасна одбрана отколку методот на автентикација со случајни битови.

4. При метод на одложена деавтентикација со интервал на одложување од 10сек, при што клиентот праќа податоци во 13-тата секунда од почетокот на деавтентикациските барања, резултат е прекин на врската и време на оправување од 21 секунда (според експериментот со напад над сите клиенти). При метод на автентикација со случајни битови, кога бројот на битови е 7, се случуваат 0.625 успешни напади во секунда и просечно време на оправување од 2.9 секунди (според експериментот).

   Во овој случај методот на автентикација со случајни битови е поефикасна одбрана отколку методот на одложена деавтентикација.

Според извршената анализа, можеме да изведеме генерален заклучок дека методот на одложена деавтентикација е поефикасен во случаите кога клиентот ги испраќа податочните рамки во периодот до 10 секунди, колку што е интервалот на одлагање, но и во третиот случај од извршената анализа, кога клиентот ги испраќа податоците во 13-тата секунда од почетокот на нападот. Од оваа анализа се гледа дека методот на одложена деавтентикација е подобар. Сепак, постојат и други фактори кои би влијаеле на ефикасноста на методите за одбрана, кои при анализата не се земени во предвид. На пример, кај првиот метод, се гледа дека различните клиенти имаат различно време на оправување од нападите, така што може да се случи времето на оправување да биде значително поголемо, што би можело да ги промени заклучоците под некои други услови.

7. ЗАКЛУЧОК

DoS и DDoS нападите се напади против достапноста, кои се обидуваат да ги спречат легалните корисници да ја користат мрежата. Поради природата на преносот во безжичните мрежи ваквите напади се лесни за спроведување,

посебно во безжичниот домен. Моменталната безжична мрежна технологија нуди малку во однос на контролата во покриената област. Ова им овозможува на напаѓачите во непосредна близина на безжична мрежа голем број на напади кои не се дел од традиналните напади кај жичните мрежи. Последиците од овие напади може да се движат од намалување на перформансите на системот, па се до негово комплетно паѓање. За да се минимизираат ризиците од напади, IT администраторите споредуваат различни мерки, вклучувајќи и безжични безбедносни политики и практики.

8. ЛИТЕРАТУРА

[1] Stuart Compton: 802.11 denial of service attacks and mitigation, SANS Institute Reading Room site, May 2007

[2] http://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack.

[3] Merrit Maxim, David Polino:Wireless security,2002

[4] http://www.interlinknetworks.com/whitepapers/Link_Layer_Security.htm

[5] Peter Egli: Susceptibility of wireless devices to denial of service attacks, Netmodule AG, 2006

[6] http://www.ogledalo.rs/mobile/networking/bezbednost/299.html

[7] Shafiullah Khan, Kok-Keong Loo, Tahir Naeem, Mohammad Abrar Khan: Denial of Service Attacks and Challenges in Broadband Wireless Networks, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.7, July 2008

[8] John Bellardo, Stefan Savage: 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions, Department of Computer Science and Engineering University of California at San Diego

[9] Kevin Beaver, Peter T. Davis: Hacking Wireless Networks for Dummies, Wiley Publishing, Inc., 2005

[10] Kemal Bicakci, Bulent Tavli: Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks, Computer Standards & Interfaces, Vol.31, (2009) 931–941

[11] http://www.sysnet.ucsd.edu/~bellardo/pubs/jsoe04-80211dos-poster.pdf

[12] Ying-Sung Lee, Hsien-Te Chien, Wen-Nung Tsai: Using Random Bit Authentication to Defend IEEE 802.11 DoS Attacks, Journal of Information Science And Engineering 25, 1485-1500 (2009)

DoS attacks on wireless networks and mitigation methods

Elena Koneska, Jasminka Sukarovska Kostadinovska, M-r Mitko Bogdanoski, Doc. D-r Saso Gelev

European University – Skopje, R. Macedonia,

koneska.elena@live.eurm.edu.mk, sukarovska.jasminka@live.eurm.edu.mk, {mitko.bogdanoski, saso.gelev}@eurm.edu.mk

Abstract – *DoS (Denial of Service) attacks are one of the biggest threats for wireless networks. DoS attack is when attacker's action causes the network to be unavailable for legitimate users, interruption or delay of services. This attack can stop all the communications in given area. DoS attacks are hard for detection and prevention. Subject of this paper is to describe DoS attacks on wireless networks, methods for mitigation and to conduct an analysis for different methods efficiency, in our case Delay Honoring Deauthentication Request method and Random Bit Authentication method.*

Keywords – DoS*, attack, attacker, wireless network, IEEE 802.11*